DATASHEET

POST-AUTHENTICATION IDENTITY GOVERNANCE

ACTIVE DIRECTORY. THE BREACH ESCALATES HERE.

87% **of 2024 breaches involved identity exploitation after valid authentication. Active Directory is the primary escalation path after the front door is already open. MFA was never designed to stop what happens next.**

– Unit 42 Incident Response Report, 2025

Agent-Based · EDR-Independent

Edge Processing on Every DC

Zero Standing Privileges

WHITESWAN
IDENTITY SECURITY

Page 02

The Problem

THE DOMAIN CONTROLLER IS THE PIVOT POINT

One compromised credential. Every system, every service account, every cloud workload with AD trust relationships becomes reachable. Traditional monitoring tools don't sit on the DC – they receive logs after the fact. By the time your SIEM fires, the attacker has already moved.

HOW AD BECOMES THE LATERAL MOVEMENT HIGHWAY

ENTRY POINT

Compromised Credential Enters AD

A valid session token or stolen credential reaches the domain controller. The attacker now operates as a legitimate identity. No perimeter tool flags this – the authentication succeeded. The attack begins here, inside your most trusted system.

Attack Vector 1

DCSync

The attacker impersonates a domain controller and triggers replication, pulling password hashes for every account in the domain. One compromised admin account is all it takes – every identity is now exposed.

⚡ WS Identity Vault AD ITDR — detects DCSync at the protocol layer on every DC, no cloud round-trip

Attack Vector 2

Pass-the-Hash / Pass-the-Ticket

Extracted NTLM hashes and Kerberos tickets allow lateral movement without ever knowing the plaintext password. The attacker moves system to system using credentials that are technically valid – your SIEM sees normal authentication events.

⚡ WS Identity Vault AD ITDR — behavioral baselines flag abnormal ticket usage and hash relay patterns in real time

Attack Vector 3

Golden Ticket

With the KRBTGT account hash, the attacker forges Kerberos tickets granting persistent access to any resource in the domain at any privilege level. This is undetectable by tools that don't sit directly on the DC – and it can persist for years.

⚡ WS Identity Vault AD ITDR — KRBTGT abuse detection with automated response, no round-trip to the cloud

Attack Vector 4

Privilege Escalation & Misconfiguration

ACL abuse, AdminSDHolder manipulation, Group Policy modification, and noPac exploits allow permanent privilege elevation without triggering standard alerts. These are configuration-layer attacks – not malware – and EDR has no visibility into any of them.

⚡ WS Identity Vault AD ITDR — continuous misconfiguration monitoring and privilege escalation detection across every DC

WHY THE CURRENT STACK FAILS

Logs arrive too late

SIEM-based AD monitoring receives event logs after the fact. DCSync, Golden Ticket, and Pass-the-Hash attacks complete in seconds. Log-based detection is structural post-breach analysis, not real-time protection.

EDR cannot see inside AD

EDR tools monitor endpoint process behavior. They have no visibility into domain controller replication traffic, Kerberos ticket anomalies, or AD object permission changes. AD attacks are identity-layer attacks – EDR operates at the endpoint layer.

Platform Capabilities

Active Directory ITDR & Protection

WS Identity Vault AD ITDR sits directly on every domain controller – processing authentication traffic at the edge, with no cloud round-trip and no dependency on any EDR vendor. Every AD attack technique is detected where it happens, in real time.

Attack Technique	How It Works	Risk	Whiteswan Detection
DCSync	Impersonates DC to replicate all password hashes	Critical	Edge replication traffic analysis on every DC
Pass-the-Hash / Pass-the-Ticket	Uses stolen NTLM hashes and Kerberos tickets for lateral movement without credentials	Critical	Hash relay detection · Ticket anomaly analysis · Behavioral baseline
Golden Ticket	Forges Kerberos tickets using KRBTGT hash – persistent access at any privilege level	Critical	KRBTGT abuse detection · Automated response
Kerberoasting	Extracts service account hashes via SPN queries	High	SPN enumeration detection · Account monitoring
ACL Abuse	Modifies AD permissions to gain persistent access	High	Continuous ACL monitoring · Change alerting
Privilege Escalation – noPac / Sam the Admin	Exploits CVE to gain domain admin via machine account	High	Privilege escalation pattern detection
Misconfiguration Abuse	Weak Group Policy, AdminSDHolder, delegation exploitation	High	Configuration drift monitoring · Policy alerting

Edge Processing Architecture

Lightweight agent on every DC catches DCSync, ticket anomalies, and escalations in real-time auth traffic at the edge – before SIEM logs.

Real-Time Threat Detection

Live authentication traffic analysis across all DC nodes simultaneously. DCSync, Pass-the-Hash, Pass-the-Ticket, and Golden Ticket attacks detected at the protocol layer – before damage propagates to the next system.

Behavioral Baseline Engine

Machine learning establishes normal patterns for every privileged account across every DC. Deviations – unusual replication requests, abnormal ticket usage, off-hours admin activity – trigger immediate alerts with full forensic context.

Automated Privilege Revocation

Unauthorized privilege escalations detected & revoked automatically, without manual incident response. The most common escalation patterns - ACL abuse, AdminSDHolder manipulation, noPac exploits are contained before completion.

Continuous Misconfiguration Monitoring

Group Policy changes, ACL modifications, AdminSDHolder abuse, and delegation drift monitored continuously across every DC. Every change is logged with full attribution and risk scoring – nothing moves without a record.

JIT Admin Access

Persistent domain admin rights eliminated entirely. Every admin session is time-bound, justified, and automatically revoked on task completion. No standing privileges. No dormant admin accounts. No lateral movement path through AD.

Forensic Audit Trails

Complete tamper-evident logging of all privileged activity across every DC in the environment. Aligned to SOX, PCI-DSS, ISO 27001, SOC 2, HIPAA & GDPR. Audit preparation reduced from weeks to days.

AD ITDR Response Lifecycle

Detect (Edge processing on DC) → **Investigate** (Behavioral context) → **Contain** (Automated revocation) → **Remediate** (Configuration restore) → **Audit** (Tamper-evident log)

Whiteswan aligns to SOX, PCI-DSS, ISO 27001, SOC 2, HIPAA & GDPR frameworks. Formal certifications are in progress.

Platform Capabilities

Conventional AD Security Tools Vs Whiteswan

Traditional SIEM and EDR vendors approach AD security from the outside – collecting logs after events complete, processing them in the cloud, and alerting after the damage is done. Whiteswan sits directly on the domain controller. There is no round-trip. There is no lag. Detection happens where the attack happens.

Capability	Whiteswan	Traditional IAM/PAM	SIEM / EDR
Edge Processing on DC (no cloud round-trip)	✓	✗	✗
DCSync Detection in Real Time	✓	Partial	✗
Golden Ticket / KRBTGT Abuse Detection	✓	Partial	✗
Pass-the-Hash / Pass-the-Ticket Detection	✓	Partial	✗
Kerberoasting Detection	✓	Partial	✗
Continuous Misconfiguration Monitoring	✓	✗	✗
JIT Admin Access (Zero Standing Privileges)	✓	✗	✗
Automated Privilege Revocation	✓	✗	✗
EDR-Independent Operation	✓	✗	N/A
Legacy OS Coverage (Win 2003–2022)	✓	Partial	✗
Deployment Time	30 Days	Weeks – Months	Weeks – Months

IMPLEMENTATION & DEPLOYMENT

⚡
30-Day Pilot
Full AD ITDR coverage live in 30 days. Edge agents deployed on domain controllers. No infrastructure overhaul, no system downtime, no dependency on existing EDR or SIEM.

🔧
Agent-Based Primary
Lightweight agents on every domain controller – Windows Server 2003 through 2022. Optional agentless gateways for constrained environments. Under 1% CPU utilization on DCs.

☁
Hybrid Deployment
On-prem AD, Azure AD / Entra ID, and hybrid environments governed from one unified policy engine. Consistent detection across every trust boundary.

🔌
Native Integrations
EDR-independent - additive to every existing security investment. Whiteswan does not replace your SIEM. It closes the gap your SIEM cannot reach.

WHITESWAN
IDENTITY SECURITY

The attackers who reach your domain controller are already past your MFA, past your EDR, and operating with valid credentials. Whiteswan detects them where they are – on the DC, in real time, independent of any other vendor in your stack.

The Domain Controller Is the Pivot Point. Govern It in 30 Days.

- **AD Risk Assessment:** Discover every misconfiguration, standing privilege, and unmonitored DC in your environment – the gaps your current stack cannot see.
- **30-Day Identity Mesh Pilot:** Edge ITDR deployed on every domain controller, JIT admin access live, and automated privilege revocation active in 30 days, without infrastructure changes.
- **ROI Analysis:** Calculate the risk reduction value of eliminating standing AD privileges and closing the DCSync, Golden Ticket, and Pass-the-Hash attack surface in your environment.

vmamidi@whiteswansecurity.com

www.whiteswansecurity.com